REMARKS

By the above amendment, Applicants have: 1) amended claims 1-5, 12, 16-17, 20-22, 24-25, 27-29, 32, and 38-40; 2) added no new claims; and 3) canceled no claims. As such, claims 1-41 are now pending. Support for the amendment is found in the specification, the drawings, and in the claims as originally filed. Applicants submit that the amendment does not add new matter. Applicants respectfully request reconsideration of the present application and consideration of the following remarks and the claims.

Claim Rejections - 35 U.S.C. § 102

"Claims 1-6 and 20-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Vogelesang, U.S. Patent No. 5,953,424."

The Office Action rejected claims 1-6 and 20-22 over Vogelesang. In particular, the Office Action rejected the independent claim 1 asserting that each and every limitation of claim 1 is met by Vogelesang. Applicants respectfully disagree.

Claim 1 currently recites:

1. A cryptographic method, including:

generating, at a first entity, a first public key M_B, the first entity having a first password P_B and the first public key M_B being session specific;

receiving, at the first entity, a second public key M_A, the second public key M_A being session specific;

generating, at the first entity, a first session key K_B based on the second public key M_A, the first public key M_B to be used at a second entity to

derive the first session key, wherein the first session key K_B is independent of the first password P_B;

encrypting, at the first entity, a first random nonce N_B using at least the first password P_B and the second public key M_A to obtain an encrypted random nonce;

transmitting the encrypted random nonce from the first entity to the second entity;

receiving a response to the encrypted random nonce; and

authenticating through determining whether the response includes a correct modification of the first random nonce.

In rejecting claim 1, the Examiner relied on Col. 16 lines 39-42 of Vogelesang for the limitation "generating, at the first entity, a first session key K_B based on the second public key M_A", Applicants respectfully disagree. The cited part of Vogelesang describes an operation for generating a shared secret (*S* in Vogelesang's notation) using an authentication factor (*K* in Vogelesang's notation) – in other words, the *S* in Vogelesang is explicitly dependent on *K* – whereas the quoted claim limitation generates "a first session key K_B", which "is independent of the first password P_B". Furthermore, Vogelesang is completely silent on "the first public key M_B to be used at a second entity to derive the first session key". Therefore, Applicants respectfully submit that claim 1 is patentable over Vogelesang since Vogelesang does not teach or suggest each and every element of the pending claim.

It should be noted that, in rejecting claim 2, which is dependent on claim 1, the Examiner relied on the exact same part of Vogelesang, that is, Col. 16 lines 39-42, for a different claim limitation included in claim 2, namely "generating a first secret S_B from at least the first

password P_B and the first public key M_B". As will be clear to people of ordinary skill in the art, embodiments of the present invention, for example, as claimed in claim 2, include two distinct elements: (a) "first session key K_B", which is "independent of the first password P_B" and (b) "a first secret S_B", which may be generated "from at least the first password P_B". Applicants respectfully submit that Vogelesang does not show both elements. Furthermore, Vogelesang is completely silent on "encrypting the first random nonce N_B using at least the first secret S_B and the first session key K_B". Therefore, Applicants respectfully submit that claim 2 is patentable over Vogelesang at least for this reason as well as for the reasons given with respect to its parent claim.

At least for the foregoing reasons, Applicants respectfully submit that claim 3 is likewise patentable over Vogelesang. Furthermore, Vogelesang is silent on the claim limitation "encrypting the first random nonce N_B using at least the first password P_B and the first session key K_B", where "[the] first session key K_B [is] based on the second public key M_A" and "the first session key K_B is independent of the first password P_B", for which the Examiner cited Col. 16 lines 64-67 of Vogelesang as a ground for the rejection. Applicants respectfully disagree. As is clearly stated in the cited part of Vogelesang, the encryption of Vogelesang does not use "at least the first password P_B and the first session key K_B". Therefore, Applicants respectfully submit that claim 3 is patentable over the prior art.

As for claims 4-6, Applicants respectfully submit that these claims are patentable over Vogelesang at least for similar reasons given with respect to claims 1-3.

Regarding claim 20-22, Applicants respectfully submit that these claims are patentable over Vogelesang at least for the foregoing reasons.

"Claims 1-2, 6-10, 20-22, 24-25, 29-31, and 38-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Wu (Wu, Thomas. The Secure Remote Password Protocol. November 11, 1997. Computer Science Department, Stanford University)."

The Office Action rejected claims 1-2, 6-10, 20-22, 24-25, 28-31, and 38-40 over Wu and it stated that the limitations of these pending claims are met by Wu. Applicants respectfully disagree. In particular, the Office Action relied upon Pages 6-7 of Wu for the claim limitations of claims 1-2 and 20-22 in rejecting these claims. Applicants respectfully disagree.

Applicants respectfully submit that Wu does not show each and every element of claim 1, claim 2, or claims 20-22. In particular, Wu is completely silent on "generating, at the first entity, a first session key K_B based on the second public key M_A". It should be noted that the symbol *K* in Wu refers to a hashed value of *S*, which depends on a password *P*, among other things, and as will be clear to one of ordinary skill in the related art, *K* of Wu is different from "first session key K_B" of embodiments of the present invention, as claimed in the claims 1-2 and 20-22. It should be further noted that "the first session key K_B is independent of the first password P_B". Please refer to the specification for examples of how "the first session key K_B" is generated in various embodiments of the present invention. (For instance, paragraphs [0065], [0082], [0123], and [0128], and FIGS. 5 and 6 of the application.)

Furthermore, among other things, Wu is completely silent on any of the following limitations: "encrypting, at the first entity, a first random nonce N_B using at least the first password P_B and the second public key M_A to obtain an encrypted random nonce",

"transmitting the encrypted random nonce from the first entity to the second entity", "receiving a response to the encrypted random nonce", or "authenticating through determining whether the response includes a correct modification of the first random nonce". Applicants respectfully request that the Examiner point out specific places in Wu where each of these limitations is disclosed.

Applicants respectfully submit that these pending claims 1-2 and 20-22 are patentable over Wu since Wu does not teach or suggest, either implicitly or explicitly, each and every element of these claims.

In rejecting claims 24-25 and 38-40, the Office Action again relied upon Pages 6-7 of Wu for the limitations of these claims. Applicants respectfully disagree.

For example, claim 24 reads:

24. A cryptographic method, comprising:

receiving at a first entity a second public key M_A and an encrypted second random number, the first entity having a first password P_B;

generating a first session key K_B based on the second public key M_A, wherein the first session key K_B is independent of the first password P_B;

decrypting, using at least the first password P_B and the first session key K_B, to retrieve a second random number N_A from the encrypted second random number;

modifying the second random number N_A to obtain a modified second random number;

encrypting the modified second random number using at least the first password P_B and the first session key K_B to obtain an encrypted random package; and

transmitting the encrypted random package from the first entity.

The Office Action rejected claim 24 asserting that Wu meets all of the limitations of this pending claim. Applicants respectfully disagree. Wu does not show each and every element of claim 24. In particular, Wu does not teach or suggest any of the following elements: "receiving ... an encrypted second random number", "generating a first session key K_B ...", "decrypting ... the encrypted second random number", "modifying the second random number N_A ...", "encrypting the modified second random number ...", or "transmitting the encrypted random package ...". Applicants respectfully request the Examiner to point out specific places where these elements are taught in Wu. Furthermore, Wu is completely silent on "the first session key K_B" which is "independent of the first password P_B". Therefore, Applicants respectfully submit that claim 24 and its dependent claim, claim 25, are patentable over Wu. As for claim 25, Wu is further silent on the limitations "decrypting the encrypted second random number using the first session key K_B to generate a first decrypted result" and "decrypting the first decrypted result using at least the first password P_B".

Applicants respectfully submit that claims 38-40 are likewise patentable over the prior art at least for similar reasons given with respect to claims 24-25.

Regarding claims 6-10 and 29-31, Applicants respectfully submit that these pending claims are patentable over Wu at least for similar reasons given in connection with claims 1 and 24 and their dependent claims.

"Claims 1-2, 6-10, 20-22, and 29-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone, U.S. Patent Application Publication No. 2001/0042205."

The Office Action rejected claims 1-2, 6-10, 20-22, and 29-31 as being anticipated by Vanstone. Applicants respectfully disagree. In rejecting these claims, the Examiner relied on paragraphs [0046]-[0062] of Vanstone for the limitations of these pending claims. Applicants respectfully disagree. Vanstone does not teach or suggest, either implicitly or explicitly, each and every element of these claims. For example, Vanstone is silent on any of the following limitations of claim 1: "encrypting, at the first entity, a first random nonce N_B using at least the first password P_B and the second public key M_A to obtain an encrypted random nonce", "transmitting the encrypted random nonce from the first entity to the second entity", "receiving a response to the encrypted random nonce", or "authenticating through determining whether the response includes a correct modification of the first random nonce". In particular, Vanstone is completely silent on "encrypting ... a first random nonce N_B using at least the first password P_B ...". Applicants respectfully request that the Examiner point out specific places where these limitations are taught in Vanstone.

Therefore, Applicants respectfully submit that claim 1 as well as claims 2, 6-10, 20-22, and 29-31 are patentable over Vanstone since Vanstone does not show each and every element of these pending claims. Applicants respectfully request reconsideration of these claims.

Claim Rejections - 35 U.S.C. § 103

"Claims 14-19, 24-27, and 33-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Schneier (Schneier, Bruce. Applied Cryptography. John Wiley & Sons. 1996. Washington DC. Pages 4-5 and 357)."

The Office Action rejected claims 14-19, 24-27, and 33-40 as being unpatentable over Vogelesang in view of Schneier. Applicants respectfully disagree.

Regarding claim 24, the Examiner asserted that "*Vogelesang discloses all the limitations of the above claim except for ...*". Applicants respectfully disagree. As stated earlier, Vogelesang is completely silent on the claim limitation "the first session key K_B" which is "independent of the first password P_B". The Examiner is once again reminded that the session key (*S* in Vogelesang's notation) of Vogelesang is explicitly dependent on the authentication factor (*K* in Vogelesang's notation). Please refer to Col. 16 lines 41-42 of Vogelesang. Furthermore, neither of the references shows the element "decrypting [the encrypted second random number] using at least the first password P_B and the first session key K_B, ...". Neither reference teaches or suggests the claim element "encrypting the modified second random number using at least the first password P_B and the first session key K_B ...". Applicants respectfully submit that Vogelesang and Schneier, either alone or combined, do not show each and every element of claim 24 and that there is no justification or motivation, in these references or in any other prior art references, to combine these references. Therefore, Applicants respectfully submit that claim 24 and claims 38-40 are patentable over these references.

Regarding claims 14-19, Applicants respectfully submit that these claims are patentable over Vogelesang in view of Schenier at least for similar reasons given with respect to the independent claim 1.

Regarding claims 25-27 and 33-37, Applicants respectfully submit that these claims are patentable over Vogelesang in view of Schenier at least for similar reasons given with respect to the independent claim 24.

"Claims 11-13, 17-19, 24, 26-32, 34-37, and 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Vanstone."

The Office Action rejected claims 11-13, 17-19, 24, 26-32, 34-37, and 38-41 over Vogelesang in view of Vanstone. Applicants respectfully disagree.

Regarding claims 11-13 and 17-19, Applicants respectfully submit that these claims are patentable over Vogelesang in view of Vanstone at least for similar reasons given with respect to the independent claim 1.

Regarding claims 24 and 38-40, Examiner stated that "*Vogelesang discloses all the limitations of the claim except ...*" and further stated that "*[i]t would have been obvious to one of ordinary skill in the art to combine the ideas of Vanstone with those of Vogelesang because doing so allows for the construction of a session key which is more secure ...*". Applicants respectfully disagree. As stated earlier, Vogelesang is completely silent on the claim limitation "the first session key K_B", which is different from the session key (S in Vogelesang's notation) of Vogelesang that is explicitly dependent on the authentication factor (K in

Vogelesang's notation). It should be noted that "the first session key K_B [is] independent of the first password P_B" in embodiments of the present invention. Furthermore, neither of the references shows the element "decrypting [the encrypted second random number] using at least the first password P_B and the first session key K_B, ...". Neither reference teaches or suggests the claim element "encrypting the modified second random number using at least the first password P_B and the first session key K_B ...". It should be further noted that Vanstone is completely silent on any of the following limitations of, for example, claim 24: "decrypting, using at least the first password P_B and the first session key K_B, to retrieve a second random number N_A from the encrypted second random number", "modifying the second random number N_A to obtain a modified second random number", "encrypting the modified second random number using at least the first password P_B and the first session key K_B to obtain an encrypted random package", or "transmitting the encrypted random package from the first entity". Applicants respectfully submit that Vogelesang and Vanstone, either alone or combined, do not show each and every element of claim 24 (or claims 38-40) and that there is no justification or motivation, in these references or in any other prior art references, to combine these references. Therefore, Applicants respectfully submit that claim 24 and claims 38-40 are patentable over these references.

Regarding claims 26-32 and 34-37, Applicants respectfully submit that these claims are patentable over Vogelesang in view of Vanstone at least for similar reasons given with respect to the independent claim 24. In particular, there is no suggestion or motivation, in either of these references or in any other prior art references other than Applicants' disclosure, to combine these references.

Regarding claim 41, Applicants respectfully submit that this claim is patentable over Vogelesang in view of Vanstone at least for similar reasons given with respect to the independent claim 40.

"Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang."

Regarding claim 23, Applicants respectfully submit that this claim is patentable over Vogelesang at least for similar reasons given with respect to the independent claim 22.

CONCLUSION

For all the above reasons, Applicants submit that the specification and claims are now in proper form, and that the claims all define patentably over the prior art. Therefore they submit that all rejections have been overcome and that all pending claims are in condition for allowance, which action they respectfully solicit. If a telephone conference would facilitate the prosecution of this application, the Examiner is invited to contact Jimmi Yoon at (408) 720-8300, extension 305.

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due or credit any overages. If an extension is required, Applicants hereby request such extension.

Respectfully Submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 3/15, 2006

H Yoon
Hyoungsoo "Jimmi" Yoon
Reg. No.: 57,637

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1030
(408) 720-8300